(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
7. Dezember 2000 (07.12.2000)

PCT

(10) Internationale Veröffentlichungsnummer
WO 00/74003 A3

(51) Internationale Patentklassifikation[7]: G07F 7/10

(21) Internationales Aktenzeichen: PCT/EP00/04781

(22) Internationales Anmeldedatum:
25. Mai 2000 (25.05.2000)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
199 24 232.1 27. Mai 1999 (27.05.1999) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, D-81677 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KOLBECK, Alexander** [DE/DE]; Merowingerstrasse 12, D-82362 Weilheim (DE).

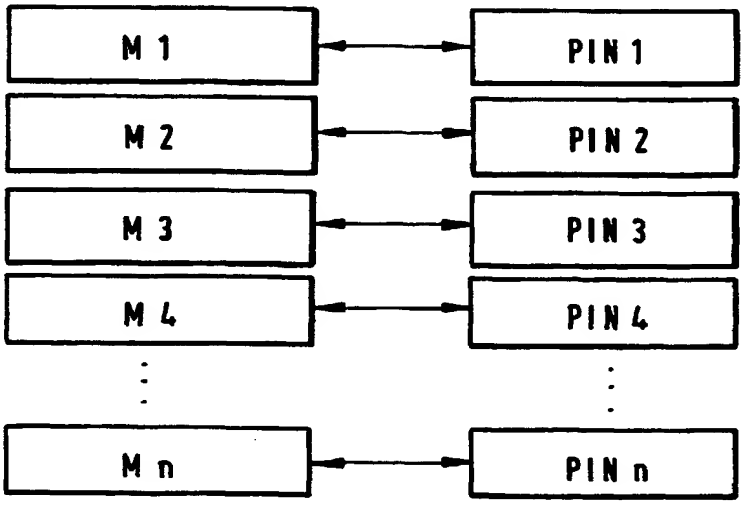
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstr. 106, D-80797 München (DE).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD AND DEVICE FOR SAVING AND RETRIEVING PIN CODES

(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUM ABSPEICHERN UND WIEDERAUFFINDEN VON PIN-CODES



(57) Abstract: The invention relates to a method and a device for saving and retrieving a number of PIN codes for devices with protected access, in particular for chip cards and magnetic strip cards. Each individual PIN code is saved, together with a unique characteristic of the respective protected-access device in a special unit, in particular in a pocket card reader. The data saved in the pocket card reader can be accessed using a user-defined access code. Whilst the access code and the unique characteristic are being input into the pocket card reader, the PIN number which has been allocated to said unique characteristic is retrieved and displayed for a short time on a display. The unique characteristic can be a serial number, which is input into the pocket card reader using a keyboard, or which is determined and used automatically by the pocket card reader. The saved unique characteristics and their respective individual PIN codes which have been allocated, can be encrypted before they are saved. The access code is stored until it is required for encryption or decryption.

[Fortsetzung auf der nächsten Seite]

WO 00/74003 A3

(84) **Bestimmungsstaaten** *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *Mit internationalem Recherchenbericht.*

(88) **Veröffentlichungsdatum des internati nalen Recherchenberichts:** 28. Juni 2001

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Es wird ein Verfahren und eine Vorrichtung zum Abspeichern und Wiederauffinden einer Anzahl von PIN-Codes für zugangsgesicherte Einrichtungen, insbesondere für Chipkarten und Magnetstreifenkarten, vorgeschlagen. Dazu werden die einzelnen PIN-Codes jeweils zusammen mit einem eindeutigen Merkmal der zugehörigen zugangsgesicherten Einrichtung in einer speziellen Vorrichtung, insbesondere in einem Taschenkartenleser, abgespeichert. Auf die in dem Taschenkartenleser abgespeicherten Daten kann mittels einem frei gewählten Zugriffscode zugegriffen werden. Indem der Zugriffscode und das eindeutige Merkmal in den Taschenkartenleser eingegeben werden, wird die dem eindeutigen Merkmal zugeordnete PIN-Nummer aufgefunden und auf einem Display für kurze Zeit angezeigt. Das eindeutige Merkmal kann eine Seriennummer sein, die über eine Tastatur in den Taschenkartenleser eingegeben wird oder von dem Taschenkartenleser automatisch ermittelt und verwendet wird. Die abgespeicherten eindeutigen Merkmale und die jeweils zugehörigen individuellen PIN-Codes können mittels des Zgriffscodes verschlüsselt werden, bevor sie abgespeichert werden. Der Zugrifffscode bleibt solange gespeichert, wie er zum Verschlüsseln oder Entschlüsseln benötigt wird.

INTERNATIONAL SEARCH REPORT

Interna[illegible]al Application No
P[illegible]EP 00/04781

A. CLASSIFICATION OF SUBJECT MATTE[illegible]
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	WO 99 56520 A (HOUSE OF ADDED VALUE AB ;SARSKOG JOHAN (SE)) 11 November 1999 (1999-11-11) page 5; claim 1 ---	1
A	EP 0 742 532 A (LENFANT JEAN PIERRE) 13 November 1996 (1996-11-13) cited in the application the whole document ---	1,14
P,A	DE 299 04 747 U (TILLMANNS FRIEDHELM) 27 May 1999 (1999-05-27) claim 1 ---	1
A	EP 0 637 004 A (NEDERLAND PTT) 1 February 1995 (1995-02-01) cited in the application claim 15 ---	1,14
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 2000	30/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Closa, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/EP 00/04781

C.(Continuation) DOCUMENTS CO ERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 606 614 A (BRADY PATRICK S ET AL) 25 February 1997 (1997-02-25) claim 1	1,14
A	DE 195 11 031 A (DEUTSCHE TELEKOM MOBIL) 2 October 1996 (1996-10-02) the whole document	1,14

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern[illegible]al Application No
P[illegible]EP 00/04781

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9956520	A	11-11-1999	SE	512671 C	17-04-2000
			AU	4300199 A	23-11-1999
			SE	9801441 A	24-10-1999
EP 0742532	A	13-11-1996	FR	2714985 A	13-07-1995
DE 29904747	U	27-05-1999	DE	19938001 A	07-09-2000
			DE	29914022 U	20-01-2000
EP 0637004	A	01-02-1995	NL	9301271 A	16-02-1995
			AT	158432 T	15-10-1997
			CA	2128355 A	21-01-1995
			DE	69405664 D	23-10-1997
			DE	69405664 T	19-03-1998
			DK	637004 T	14-04-1998
			EP	0775991 A	28-05-1997
			ES	2107090 T	16-11-1997
			GR	3025686 T	31-03-1998
			US	5914471 A	22-06-1999
US 5606614	A	25-02-1997	CA	2171345 A	20-04-1995
			DE	69409972 D	04-06-1998
			DE	69409972 T	10-09-1998
			EP	0740819 A	06-11-1996
			ES	2117303 T	01-08-1998
			WO	9510823 A	20-04-1995
			HU	74344 A	30-12-1996
			JP	9503877 T	15-04-1997
			SG	49729 A	15-06-1998
DE 19511031	A	02-10-1996	NONE		

INTERNATIONALER RECHERCHENBERICHT

Interna[illegible]ales Aktenzeichen
P[illegible]P 00/04781

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F G06K

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P,X	WO 99 56520 A (HOUSE OF ADDED VALUE AB ;SARSKOG JOHAN (SE)) 11. November 1999 (1999-11-11) Seite 5; Anspruch 1	1
A	EP 0 742 532 A (LENFANT JEAN PIERRE) 13. November 1996 (1996-11-13) in der Anmeldung erwähnt das ganze Dokument	1,14
P,A	DE 299 04 747 U (TILLMANNS FRIEDHELM) 27. Mai 1999 (1999-05-27) Anspruch 1	1
A	EP 0 637 004 A (NEDERLAND PTT) 1. Februar 1995 (1995-02-01) in der Anmeldung erwähnt Anspruch 15	1,14

-/--

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
23. November 2000	30/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Closa, D

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Interna ales Aktenzeichen
PCT/EP 00/04781

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 606 614 A (BRADY PATRICK S ET AL) 25. Februar 1997 (1997-02-25) Anspruch 1	1,14
A	DE 195 11 031 A (DEUTSCHE TELEKOM MOBIL) 2. Oktober 1996 (1996-10-02) das ganze Dokument	1,14

Formblatt PCT/ISA/210 (Fortsetzung von Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Interna les Aktenzeichen
PC EP 00/04781

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
WO 9956520	A	11-11-1999	SE	512671 C	17-04-2000
			AU	4300199 A	23-11-1999
			SE	9801441 A	24-10-1999
EP 0742532	A	13-11-1996	FR	2714985 A	13-07-1995
DE 29904747	U	27-05-1999	DE	19938001 A	07-09-2000
			DE	29914022 U	20-01-2000
EP 0637004	A	01-02-1995	NL	9301271 A	16-02-1995
			AT	158432 T	15-10-1997
			CA	2128355 A	21-01-1995
			DE	69405664 D	23-10-1997
			DE	69405664 T	19-03-1998
			DK	637004 T	14-04-1998
			EP	0775991 A	28-05-1997
			ES	2107090 T	16-11-1997
			GR	3025686 T	31-03-1998
			US	5914471 A	22-06-1999
US 5606614	A	25-02-1997	CA	2171345 A	20-04-1995
			DE	69409972 D	04-06-1998
			DE	69409972 T	10-09-1998
			EP	0740819 A	06-11-1996
			ES	2117303 T	01-08-1998
			WO	9510823 A	20-04-1995
			HU	74344 A	30-12-1996
			JP	9503877 T	15-04-1997
			SG	49729 A	15-06-1998
DE 19511031	A	02-10-1996	KEINE		

Verfahren und Vorrichtung zum Abspeichern und Wiederauffinden von PIN-Codes

Die Erfindung betrifft ein Verfahren und eine Vorrichtung zum Abspeichern und Wiederauffinden einer Anzahl von persönlichen Identifikationsnummern (PINs) für zugangsgesicherte Einrichtungen, insbesondere für Chip- und Magnetstreifenkarten.

Heutzutage sind viele Einrichtungen durch persönliche Identifikationsnummern zugangsgesichert. PINs werden insbesondere für Chipkarten, Geldkarten, Ausweiskarten aber auch für zugangsgeschützte Software und dergleichen vergeben. Erst nach Angabe des jeweiligen PIN-Codes ist der Zugang möglich. Die PINs muß sich der PIN-Inhaber merken, damit nur er davon Kenntnis haben kann. Die ständig steigende Anzahl der sich zu merkenden PINs stellt ein Problem dar, da die menschliche Merkfähigkeit begrenzt ist und die PINs zumeist nicht frei wählbar und daher nur schwierig zu merken sind.

Aus der EP-A-0 742 532 sind ein Verfahren und eine Vorrichtung zum einfachen und sicheren Abspeichern und Wiederauffinden von PIN-Codes bekannt. Dort wird vorgeschlagen, den geheimen PIN-Code in einen nicht von außen auslesbaren Primärspeicher einzuspeichern und einen für den PIN-Code-Inhaber leichter merkbaren persönlichen Code, der frei wählbar ist, in einen Sekundärspeicher einzuspeichern. Wenn der PIN-Code-Inhaber den geheimen PIN-Code vergessen hat, gibt er den persönlichen Code in die Vorrichtung ein, und wenn ein in einem Mikroprozessor durchgeführter Vergleich mit dem im Sekundärspeicher abgespeicherten persönlichen Code übereinstimmt, dann wird auf einem Display für eine vorgegebene Zeitspanne der im Primärspeicher abgespeicherte geheime PIN-Code angezeigt.

Es können auch mehrere geheime PIN-Codes in dem Primärspeicher abgespeichert werden, die mittels demselben persönlichen Code nacheinander auf dem Display angezeigt werden. In der EP-A-0 637 004 ist am Ende der Beschreibungseinleitung ebenfalls ein solches Verfahren offenbart.

Die im Stand der Technik vorgeschlagenen Lösungen haben den Nachteil, daß sich der Inhaber mehrerer geheimer PIN-Codes neben dem leichter merkfähigen persönlichen Code zumindest noch merken muß, welcher Chip- oder Magnetkarte die gespeicherten und wiederaufgefundenen geheimen PIN-Codes jeweils zuzuordnen sind. Bei der ständig zunehmenden Anzahl von durch PINs zugangsgesicherten Einrichtungen kann diese vorgeschlagene Lösung nicht befriedigen.

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren und eine Vorrichtung zum Abspeichern und Wiederauffinden einer Anzahl von PIN-Codes vorzuschlagen, bei denen mittels einem einzigen, frei wählbaren persönlichen Code genau derjenige geheime PIN-Code wiederaufgefunden werden kann, der der jeweiligen zugangsgesicherten Einrichtung zugehörig ist.

Die Erfindung wird durch die Merkmale der nebengeordneten Ansprüche gelöst.

Im Gegensatz zu den bekannten Systemen zum Abspeichern und Wiederauffinden einer Anzahl von PIN-Codes wird erfindungsgemäß zusätzlich zu jedem abgespeicherten PIN-Code ein eindeutiges Merkmal der jeweils zugehörigen zugangsgesicherten Einrichtung, beispielsweise die Seriennummer einer Chipkarte oder eine automatisch gemessene Eigenschaft des in der Chipkarte enthaltenen Chips, abgespeichert. Dabei wird zwischen jedem abgespeicherten PIN-Code und dem zugehörigen abgespeicherten eindeuti-

gen Merkmal der jeweiligen Einrichtung bzw. Chipkarte eine eindeutige feste Verknüpfung erzeugt. Beim Wiederauffinden eines individuellen PIN-Codes für eine zugangsgesicherte Einrichtung werden dann zwei Angaben gemacht, nämlich einerseits wird ein zuvor frei gewählter Zugriffscode angegeben, der für jeden Wiederauffindungsvorgang derselbe und daher leicht merkbar ist. Andererseits wird das eindeutige Merkmal der zugangsgesicherten Einrichtung bzw. Chipkarte angegeben, deren individueller PIN wiederaufgefunden werden soll. Der Zugriffscode, der nur dem Inhaber der individuellen PIN bekannt ist, stellt sicher, daß die individuellen PINs nicht von Dritten ausgespäht werden können. Die Angabe des eindeutigen Merkmals wird benötigt, um über die eindeutige feste Verknüpfung den zugehörigen individuellen PIN wiederaufzufinden. Der individuelle wiederaufgefundene PIN kann sodann angezeigt werden.

Das erfindungsgemäße Verfahren und die Vorrichtung bieten somit durch die jeweilige Verknüpfung der geheimen PIN-Codes mit dem eindeutigen Merkmal der zugehörigen zugangsgesicherten Einrichtung den Vorteil, daß mittels eines einzigen, frei wählbaren Zugriffscodes die sichere Verwahrung und zielgenaue Wiederauffindung verschiedener PIN-Codes möglich ist.

Beim Wiederauffinden des PIN-Codes ist es irrelevant, ob zunächst der frei gewählte Zugriffscode oder das eindeutige Merkmal angegeben wird. Der individuelle PIN wird in jedem Falle erst dann ausgegeben, wenn sowohl der angegebene Zugriffscode zulässig war als auch das angegebene eindeutige Merkmal mit einem der abgespeicherten eindeutigen Merkmale übereinstimmt.

Vorteilhafterweise werden der Zugriffscode und/oder die eindeutigen Merkmale und/oder die PIN-Codes in verschlüsselter Form abgespeichert.

Dies erschwert es einem Dritten, der sich Zugang zu den Speicherbereichen verschafft hat, die relevanten Inhalte der Speicher zu erfassen.

In einer besonderen Ausführungsform des Verfahrens ist vorgesehen, daß der Zugriffscode als Schlüssel zur Verschlüsselung der eindeutigen Merkmale und/oder PIN-Codes dient und nur solange gespeichert bleibt, wie er zur Verschlüsselung dieser Daten benötigt wird. Beim Wiederauffinden eines individuellen PINs wird das eindeutige Merkmal derjenigen Einrichtung, dessen individueller PIN wiederaufgefunden werden soll, angegeben und mittels dem ebenfalls anzugebenden Zugriffscode verschlüsselt, wobei anschließend ein Vergleich mit den zuvor abgespeicherten und identisch verschlüsselten eindeutigen Merkmalen erfolgt. Durch den Vergleich des verschlüsselten angegebenen Merkmals mit dem verschlüsselt abgespeicherten Merkmal werden somit zwei Prüfungen gleichzeitig durchgeführt, nämlich einerseits, ob der Zugriffscode zulässig ist und andererseits, ob das angegebene eindeutige Merkmal mit einem der abgespeicherten eindeutigen Merkmale übereinstimmt. Denn wenn der Zugriffscode nicht zulässig ist oder ein entsprechendes eindeutiges Merkmal nicht abgespeichert ist, fällt der Vergleich negativ aus.

Im Falle, daß der Vergleich negativ ausfällt, wird ein falscher, nicht abgespeicherter PIN-Code ausgegeben. Fällt der Vergleich positiv aus, so wird der verschlüsselt abgespeicherte individuelle PIN-Code mit dem angegebenen Zugriffscode wieder entschlüsselt und ausgegeben. Anschließend wird der Zugriffscode wieder gelöscht.

Um die Sicherheit der abgespeicherten Daten vor unerlaubtem Zugriff zu erhöhen, können die PIN-Codes auch - und gegebenenfalls zusätzlich zu der zuvor beschriebenen Verschlüsselung - verschlüsselt werden, indem das je-

weils eindeutige Merkmal der dem PIN-Code zugehörigen zugangsgesicherten Einrichtung den Schlüssel bildet.

Die PIN-Codes werden dann am sichersten verwahrt, wenn der frei gewählte Zugriffscode nur kurzzeitig abgespeichert wird, also nach dem Löschen nicht mehr vorliegt, die abgespeicherten eindeutigen Merkmale mit dem Zugriffscode verschlüsselt vorliegen und die jeweils zugehörigen PIN-Codes einerseits mit dem Zugriffscode und andererseits mit dem zugehörigen verschlüsselten eindeutigen Merkmal verschlüsselt vorliegen. Die Entschlüsselung und nachfolgende Ausgabe der PIN-Codes erfolgt dann in umgekehrter Reihenfolge allein durch Angabe des Zugriffscodes und des jeweiligen eindeutigen Merkmals der zugriffsgesicherten Einrichtung, deren individueller PIN-Code wiederaufgefunden werden soll.

Als zugangsgesicherte Einrichtungen kommen insbesondere Chipkarten und Magnetstreifenkarten in Betracht. Als eindeutiges Merkmal einer Magnetstreifenkarte kommt beispielsweise deren Seriennummer in Betracht, die zusätzlich zum Zugriffscode manuell angegeben werden muß. Insbesondere bei Chipkarten kommt neben der Seriennummer als eindeutiges Merkmal auch eine für den jeweiligen Chip charakteristische physikalische Eigenschaft in Betracht. Eine solche physikalische Eigenschaft kann beispielsweise die für einen jeden Chip charakteristische Datenverarbeitungsgeschwindigkeit sein, die anhand eines definierten Algorithmus ermittelt wird. Die Zeitspanne, die der Chip benötigt, um den vorgegebenen Algorithmus auszuführen, dient dann als eindeutiges Merkmal für die Chipkarte.

Das erfindungsgemäße Verfahren kann vorteilhafter Weise mit einem modifizierten Taschenkartenleser durchgeführt werden. Taschenkartenleser werden dazu verwendet, die frei zugänglichen, fest in eine Chipkarte eingespeicherten oder veränderbaren Daten auszulesen. Insbesondere im Zusammen-

hang mit Geldkarten werden sie eingesetzt, um zu verifizieren, welcher Geldbetrag auf der Geldkarte noch gespeichert ist. Solche herkömmlichen Taschenkartenleser werden lediglich mit einer Tastatur zur Eingabe des frei gewählten Zugriffscodes und der abzuspeichernden PIN-Codes sowie gegebenenfalls der Seriennummern oder anderer eindeutiger Merkmale der zugehörigen Karten ausgerüstet, sowie mit einer Software zur Durchführung des zuvor beschriebenen Verfahrens zum Ausgeben und Wiederauffinden der PIN-Codes. Falls das eindeutige Merkmal eine charakteristische physikalische Eigenschaft der Karte ist, die automatisch erfaßt wird, ist der Taschenkartenleser mit einer entsprechenden Einrichtung ausgestattet. Das heißt beispielsweise, daß der Taschenkartenleser ein Programm und eine Einrichtung enthält, mit denen ein Algorithmus auf der Chipkarte ausgeführt und die Zeitdauer für die Ausführung des Algorithmus gemessen wird.

Die Verwendung eines Taschenkartenlesers hat den Vorteil, daß er sehr flach ist und etwa die Größe einer Chipkarte hat, so daß er jederzeit mitgeführt werden kann.

Nachfolgend wird die Erfindung beispielhaft anhand der beiden Figuren erläutert. Darin zeigen:

Figur 1 eine Chipkarte 10 und einen Taschenkartenleser 20, in den die Chipkarte 10 eingeführt werden kann, und

Figur 2 die Verknüpfung zwischen Speicherbereichen Ml bis Mn, die Daten zu eindeutigen Merkmalen enthalten, jeweils mit einem zugeordneten Speicherbereich PIN1 bis PINn, in denen die geheimen PIN-Codes abgespeichert sind.

Figur 1 zeigt eine Chipkarte 10 mit einem Chipmodul 12, einem Schriftfeld 11 und einer Seriennummer 13. Die Chipkarte kann eine Geldkarte oder eine Kreditkarte oder dergleichen sein, und vor jedem Zugriff auf einen geheimen Speicherbereich des Chips in dem Chipmodul 12 der Chipkarte 10 ist die Angabe eines geheimen PIN-Codes erforderlich. Die Karte kann in den Taschenkartenleser 20, der ein wenig breiter als die Chipkarte 10 ist, eingeschoben werden. Dazu weist der Taschenkartenleser 20 zwei plattenartige Deckelemente 21 und 22 auf, die an ihren Kanten 24 miteinander verbunden sind und zwischen sich einen Spalt 23 bilden, in den die Chipkarte 10 eingeführt wird, wie mit dem Pfeil in Figur 1 dargestellt. Handelt es sich um eine Geldkarte, so zeigen herkömmliche Taschenkartenleser den auf der Geldkarte gespeicherten Geldbetrag an, ohne daß es der Eingabe eines PIN-Codes bedarf. Wenn der Benutzer der Geldkarte an einem Bankautomaten den auf der Karte gespeicherten Geldbetrag aufstocken möchte, muß er in den Bankautomaten zunächst seine persönliche PIN eingeben, um die Transaktion starten zu können. Dieser PIN-Code kann der Karteninhaber mit vielen weiteren PIN-Codes in dem Taschenkartenleser derart speichern, daß er sie jederzeit wiederauffinden kann, beispielsweise wenn er eine Transaktion zum Auffüllen der Geldkarte vornehmen möchte.

Das Verfahren zum Einspeichern und Wiederauffinden einer Anzahl von PIN-Codes wird nun beispielhaft an dem Taschenkartenleser 20 beschrieben.

Zunächst wird durch Drücken der Taste IN dem Taschenkartenleser 20 angezeigt, daß ein frei wählbarer Zugriffscode eingegeben werden soll. Der frei wählbare Zugriffscode wird sinvollerweise bei der Inbetriebnahme des Taschenkartenlesers 20 eingegeben. Es kann auch vorgesehen sein, daß mehrere Benutzer mit jeweils mehreren Chipkarten einen Taschekartenleser verwenden. Dann werden mehrere Zugriffscodes verwendet, d. h. mindestens ein Zugriffscode pro Benutzer.

Daraufhin wird mit Hilfe der numerischen oder alphanumerischen Tastatur 26 die frei wählbare PIN eingegeben und anschließend durch erneutes Drükken der Taste IN bestätigt. Die frei wählbare PIN wird zumindest für einen kurzen Zeitraum abgespeichert und fortan als Zugriffscode für den Taschenkartenleser verwendet.

Als nächstes wird ein eindeutiges Merkmal der Chipkarte 10 in den Taschenkartenleser eingegeben und durch Drücken der Taste IN bestätigt. Als eindeutiges Merkmal kann beispielsweise die Seriennummer 13 der Chipkarte 10 verwendet werden. Nach Eingabe des eindeutigen Merkmals wird die der Chipkarte 10 gespeicherte geheime PIN in den Taschenkartenleser eingegeben und ebenfalls durch Drücken der Taste IN bestätigt. Es kann auch zunächst die geheime PIN und anschließend das eindeutige Merkmal der Chipkarte 10 eingegeben werden. In jedem Falle führt das Display 25 den Benutzer durch das Programm, indem es anzeigt, welche Information als nächstes einzugeben ist. In Figur 1 ist im Display 25 dargestellt, daß als nächstes der geheime PIN-Code einzugeben ist, der einen ersten Speicherbereich PIN1 belegt, wie nachfolgend erläutert.

In Figur 2 sind Speicherbereiche Ml bis Mn und PIN1 bis PINn angegeben. Das eingegebene eindeutige Merkmal der Chipkarte 10, im Beispielsfall die Seriennummer 13 der Chipkarte 10, wird im Speicherbereich Ml abgespeichert und die zugehörige PIN wird im Speicherbereich PIN 1 abgespeichert. Beide Speicherbereiche sind fest miteinander verknüpft, wie durch den Doppelpfeil angedeutet wird. Damit ist der Abspeichervorgang abgeschlossen. Auf die beschriebene Weise können weitere eindeutige Merkmale M2 bis Mn mit fest zugeordneten persönlichen Identifikationsnummern PIN2 bis PINn abgespeichert werden. Die Speicherbereiche Ml bis Mn und PIN1 bis

PINn sind von außen nicht zugänglich bzw. nicht auslesbar. Dies gilt auch für den Speicherbereich in dem der Zugriffscode gespeichert ist.

Das Wiederauffinden eines speziellen abgespeicherten PINs erfolgt in analoger Weise. Durch Drücken der Taste OUT wird dem Taschenkartenleser 20 angezeigt, daß ein individueller PIN ausgelesen werden soll. Der Taschenkartenleser 20 fordert den Benutzer dann auf, einerseits den Zugriffscode anzugeben und andererseits das eindeutige Merkmal der Chipkarte anzugeben, deren individueller PIN-Code wiederaufgefunden werden soll. Im oben beschriebenen Beispielsfall wird als eindeutiges Merkmal die Seriennummer 13 der Chipkarte 10 angegeben. Nachdem der Taschenkartenleser 20 die Zulässigkeit des Zugriffcodes geprüft und bestätigt hat und nachdem im Taschenkartenleser 20 ein Vergleich des angegebenen Merkmals mit den in den Speicherbereichen Ml bis Mn abgespeicherten eindeutigen Merkmalen ein positives Ergebnis geliefert hat, wird auf dem Display 25 der zu dem aufgefundenen eindeutigen Merkmal zugehörige individuelle PIN-Code angezeigt, im Beispielsfalle also der im Speicherbereich PIN 1 abgespeicherte PIN-Code. Das Display erlischt nach einigen Sekunden, beispielsweise etwa nach 3 Sekunden, oder nachdem die Karte dem Taschenkartenleser wieder entzogen wurde.

Falls entweder der angegebene Zugriffscode unzulässig war oder zu dem angegebenen eindeutigen Merkmal kein abgespeichertes eindeutiges Merkmal auffindbar ist, wird in dem Display 25 ein PIN-Code angezeigt, der mit keinem der in den Speicherbereichen PIN1 bis PINn abgespeicherten PIN-Codes übereinstimmt, wahlweise wird eine Fehlermeldung angezeigt.

In der zuvor beschriebenen Ausführungsform ist ein eindeutiges Merkmal einer Chipkarte mit der dieser Chipkarte zugehörigen PIN verknüpft, indem die jeweiligen Speicherbereiche Ml und PIN1, M2 und PIN2, ... Mn und PINn

einander fest zugeordnet sind. In einer alternativen Ausführungsform erfolgt die Verknüpfung der Daten, indem jede abgespeicherte geheime PIN mit dem zugehörigen eindeutigen Merkmal verschlüsselt wird. Beim Versuch des Wiederauffindens der verschlüsselt abgespeicherten PIN wird die verschlüsselt abgespeicherte PIN mittels demselben eindeutigen Merkmal entschlüsselt. Die verknüpften Speicherbereiche sind somit nicht fest verdrahtet sondern logisch miteinander verknüpft.

Nach einer weiteren Ausgestaltung der Erfindung ist vorgesehen, daß der frei gewählte Zugriffscode nur temporär gespeichert wird. Der Zugriffscode muß nur solange gespeichert bleiben, wie er beim Abspeichern von individuellen PINs zur Verschlüsselung des zugehörigen eindeutigen Merkmals und gegebenenfalls des individuellen PINs benötigt wird. Nach dem Eingeben eines eindeutigen Merkmals und des zugehörigen PINs, dem Verschlüsseln des eindeutigen Merkmals und gegebenenfalls des individuellen PINs mit dem Zugriffscode sowie dem Abspeichern des verschlüsselten eindeutigen Merkmals und gegebenenfalls verschlüsselten individuellen PINs liegen das eindeutige Merkmal und der individuelle PIN in den jeweiligen Speicherbereichen verschlüsselt vor, während der als Schlüssel verwendete Zugriffscode wieder gelöscht wird. Dadurch wird sichergestellt, daß jemand, der sich ohne Kenntnis des Zugriffscodes Zugang zu den einzelnen Speicherbereichen verschaffen konnte, die Inhalte der Speicherbereiche nicht interpretieren kann.

Zu Beginn des Wiederauffindens einer individuellen PIN wird der Zugriffscode und das eindeutige Merkmal der Chipkarte, deren individueller PIN wiederaufgefunden werden soll, über die Tastatur 26 eingegeben. Sodann wird das eingegebene eindeutige Merkmal mit dem Zugriffscode verschlüsselt und anschließend wird geprüft, ob es zu dem derart verschlüsselten eindeutigen Merkmal ein Pendant in den Speicherbereichen Ml bis Mn gibt, in

denen die eindeutigen Merkmale verschiedener Chipkarten zuvor verschlüsselt abgespeichert wurden. Ergibt diese Prüfung ein positives Ergebnis, so wird der damit verknüpfte PIN-Code, gegebenenfalls nach Entschlüsselung mittels des Zugriffscodes, auf dem Display 25 angezeigt.

Die Karte 10 muß keine Chipkarte sein, sondern kann beispielsweise auch eine Magnetstreifenkarte sein. Die Erfindung ist darauf in gleicher Weise anwendbar. Wenn es sich jedoch um eine Chipkarte handelt, bietet sich ein automatisiertes Verfahren zur Angabe des eindeutigen Merkmals an. Anstelle der Eingabe eines eindeutigen Merkmals wie der Seriennummer über die Tastatur 26, kann der Taschenkartenleser auch eine charakteristische Eigenschaft oder Seriennummer des in der Chipkarte 10 enthaltenen Chips 12 automatisch ermitteln und als eindeutiges Merkmal verwenden. Im Falle von Geldkarten beispielsweise erfolgt ohnehin ein Datentransfer zwischen dem Taschenkartenleser 20 und dem Chip 12 der Chipkarte 10, um den in der Chipkarte gespeicherten Geldbetrag anzeigen zu können. Es ist daher problemlos möglich, eine charakteristische physikalische Eigenschaft des Chips über die ohnehin realisierte Kontaktierung zwischen Chip 12 und Taschenkartenleser 20 zu ermitteln. Dazu veranlaßt der Taschenkartenleser 20 in dem Chip 12 die Durchführung eines Algorithmus und die Zeitdauer, die der Chip 12 benötigt, um den Algorithmus abzuarbeiten, wird erfaßt und als charakteristische physikalische Eigenschaft des Chips 12 und somit der Chipkarte 10 verwendet. Dieser Vorgang erfolgt automatisch nachdem die Chipkarte 10 in den Spalt 23 des Taschenkartenlesers 20 vollständig eingeschoben worden ist und der Benutzer des Taschenkartenlesers durch Drükken der Taste OUT anzeigt, daß er die dieser Chipkarte zugehörige individuelle PIN wiederauffinden möchte. Der Karteninhaber muß nur noch den zuvor frei gewählten Zugriffscode über die Tastatur 26 in den Taschenkartenleser 20 eingeben, um das zuvor beschriebene Vergleichsverfahren der charakteristischen physikalischen Eigenschaft zu starten und die Anzeige

des der Karte 10 zugehörigen individuellen PINs auf dem Display 25 zu erhalten. Als charakteristische physikalische Eigenschaft kann jede Eigenschaft dienen, die zuverlässig erfaßbar und für jede Karte bzw. ihren Chip individuell ist.

Prinzipiell ist das oben für eine Chipkarte beschriebene automatische Verfahren zur Ermittlung des eindeutigen Merkmals auch bei einer Magnetstreifenkarte möglich, die auch über eindeutige Merkmale wie Seriennummern verfügt. Allerdings ist der Aufbau eines geeigneten Taschkartenlesers aufwendiger als in dem oben für eine Chipkarte beschriebenen Fall.

Patentansprüche

1. Verfahren zum Abspeichern und Wiederauffinden einer Anzahl von PIN-Codes für zugangsgesicherte Einrichtungen, umfassend Schritte zum Abspeichern der PIN-Codes, nämlich
   - Angeben und zumindest kurzzeitiges Abspeichern eines Zugriffscodes,
   - Angeben und Abspeichern von mindestens einem PIN-Code einer zugangsgesicherten Einrichtung,
   - Angeben und Abspeichern von mindestens einem eindeutigen Merkmal mindestens einer zugangsgesicherten Einrichtung,
   - Herstellen einer Verknüpfung zwischen jeweils einem der abgespeicherten PIN-Codes und dem abgespeicherten eindeutigen Merkmal derjenigen Einrichtung, die mit dem betreffenden PIN-Code zugangsgesichert ist, und

   Schritte zum Wiederauffinden eines bestimmten abgespeicherten PIN-Codes, nämlich
   - Angeben des Zugriffscodes,
   - Angeben des eindeutigen Merkmals der zu dem wiederaufzufindenden PIN-Code gehörigen zugangsgesicherten Einrichtung,
   - Prüfen, ob der Zugriffscode zulässig ist,
   - Prüfen, ob das angegebene eindeutige Merkmal mit einem der abgespeicherten eindeutigen Merkmale übereinstimmt, und
   - wenn beide Prüfungen positiv ausfallen, Ausgeben des mit dem eindeutigen Merkmal verknüpften, abgespeicherten PIN-Codes.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, daß der abgespeicherte Zugriffscode dauerhaft abgespeichert wird und die Prüfung

der Zulässigkeit des angegebenen Zugriffscodes anhand eines Vergleichs mit dem dauerhaft abgespeicherten Zugriffscode erfolgt.

3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch **gekennzeichnet**, daß der Zugriffscode und/oder die eindeutigen Merkmale und/oder die PIN-Codes in verschlüsselter Form abgespeichert werden.

4. Verfahren nach Anspruch 3, dadurch **gekennzeichnet**, daß der Zugriffscode als Schlüssel für das verschlüsselte Abspeichern verwendet wird.

5. Verfahren nach Anspruch 4, dadurch **gekennzeichnet**, daß der Zugriffscode nur kurzzeitig abgespeichert wird und gelöscht wird, nachdem die Verschlüsselung erfolgt ist.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, daß die Verknüpfung zwischen dem eindeutigen Merkmal einer zugangsgesicherten Einrichtung und dem zugehörigen PIN-Code durch eine Verschlüsselung des PIN-Codes erfolgt, wobei das eindeutige Merkmal den Schlüssel bildet.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, daß der Zugriffscode und/oder die eindeutigen Merkmale und/oder die PIN-Codes in von außen unzugänglichen Speicherbereichen abgespeichert werden.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, daß als eindeutiges Merkmal die jeweilige Seriennummer der zugangsgesicherten Einrichtung verwendet wird.

9. Verfahren nach einem der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, daß als eindeutiges Merkmal eine charakteristische physikalische Eigenschaft der zugangsgesicherten Einrichtung verwendet wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch **gekennzeichnet**, daß das jeweilige eindeutige Merkmal automatisch ermittelt und angegeben wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch **gekennzeichnet**, daß die Ausgabe des PIN-Codes nur über einen begrenzten Zeitraum zur Verfügung gestellt wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch **gekennzeichnet**, daß die zugangsgesicherten Einrichtungen Chipkarten und/oder Magnetstreifenkarten sind.

13. Verfahren nach einem der Ansprüche 1 bis 12, dadurch **gekennzeichnet**, daß ein falscher, nicht abgespeicherter PIN-Code ausgegeben wird, wenn eine der beiden Prüfungen negativ ausfällt.

14. Vorrichtung (20) zum Abspeichern und Wiederauffinden einer Anzahl von PIN-Codes für zugangsgesicherte Einrichtungen (10), umfassend
- eine Tastatur (26) zur Angabe der PIN-Codes und eines Zugriffscodes,
- eine Einrichtung zum Empfangen eines jeweils eindeutigen Merkmals der zugangsgesicherten Einrichtungen (10),
- mindestens einen Speicher zum zumindest kurzzeitigen Abspeichern des Zugriffscodes, zum Abspeichern der PIN-Codes und zum Abspeichern der eindeutigen Merkmale,

- eine Einrichtung zum Prüfen eines angegebenen Zugriffscodes auf seine Zulässigkeit und zum Vergleichen eines angegebenen eindeutigen Merkmals mit abgespeicherten eindeutigen Merkmalen und
- ein Display (25) zum Anzeigen wiederaufgefundener PIN-Codes.

15. Vorrichtung nach Anspruch 14, dadurch **gekennzeichnet**, daß die Vorrichtung (20) ein Taschenkartenleser ist.

16. Vorrichtung nach Anspruch 13 oder 14, dadurch **gekennzeichnet**, daß eine Einrichtung zum Verschlüsseln der PIN-Codes und/oder der eindeutigen Merkmale und/oder des Zugriffscodes vorgesehen ist.

17. Vorrichtung nach einem der Ansprüche 14 bis 16, dadurch **gekennzeichnet**, daß von außen nicht zugängliche Speicherbereiche zum Abspeichern der PIN-Codes und/oder der eindeutigen Merkmale und/oder des Zugriffscodes vorgesehen sind.

18. Vorrichtung nach einem der Ansprüche 14 bis 17, dadurch **gekennzeichnet**, daß die Tastatur (26) die Einrichtung zum Empfangen der eindeutigen Merkmale bildet.

19. Vorrichtung nach einem der Ansprüche 14 bis 17, dadurch **gekennzeichnet**, daß die Einrichtung zum Empfangen der eindeutigen Merkmale eine Einrichtung zum automatischen Ermitteln der eindeutigen Merkmale der zugriffsgeschützten Einrichtungen umfaßt.